



# Lecture 2: Examples of Poor Engineering

## → "Software Forensics" Case Studies:

- ↳ Mars Pathfinder
- ↳ Mars Climate Observer
- ↳ Mars Polar Lander
- ↳ Deep Space 2

## → Some conclusions

- ↳ e.g. Reliable software has very little to do with writing good programs
- ↳ e.g. Humans make mistakes, but good engineering practice catches them!



# NASA JPL's Mars Program

Mission	Launch Date	Arrival Date	Outcome
Viking I Viking II	20 Aug 1975 9 Sept 1975	Landed 20 Jul 1976 Landed 3 Sept 1976	Operated until 1982 Operated until 1980
Mars Observer	25 Sept 1992	Last contact: 22 Aug 1993	Contact lost just before orbit insertion
Pathfinder	4 Dec 1996	Landed 4 July 1997	Operated until 27 Sept 1997
Global Surveyor	7 Nov 1996	Orbit attained 12 Sept 1997	Still operational
Climate Orbiter	11 Dec 1998	Last contact: 23 Sept 1999	Contact lost just before orbit insertion
Polar Lander	3 Jan 1999	Last contact: 3 Dec 1999	Contact lost before descent
Deep Space 2	3 Jan 1999	Last contact: 3 Dec 1999	No data was ever retrieved
Mars Odyssey	7 Apr 2001	Expected: October 24, 2001	



# Mars Pathfinder

## → Mission

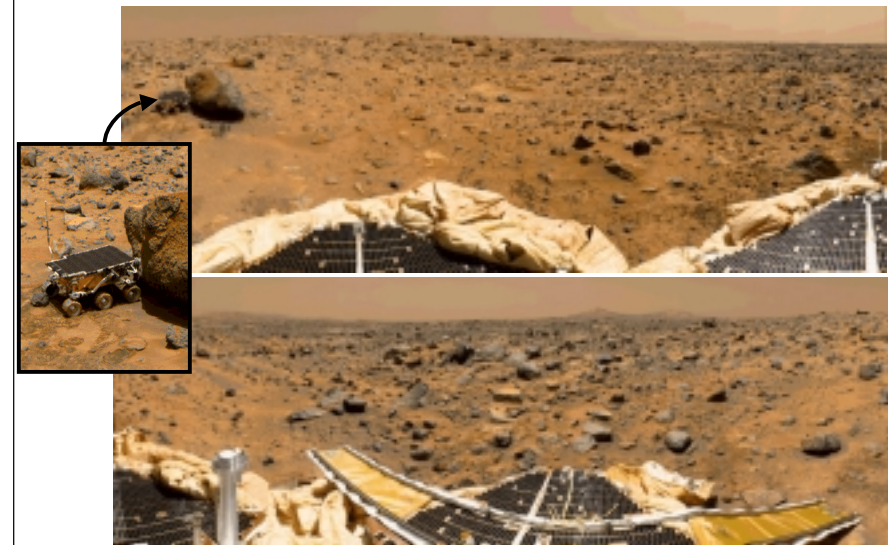
- ↳ Demonstrate new landing techniques
  - ↳ parachute and airbags
- ↳ Take pictures
- ↳ Analyze soil samples
- ↳ Demonstrate mobile robot technology
  - ↳ Sojourner

## → Major success on all fronts

- ↳ Returned 2.3 billion bits of information
- ↳ 16,500 images from the Lander
- ↳ 550 images from the Rover
- ↳ 15 chemical analyses of rocks & soil
- ↳ Lots of weather data
- ↳ Both Lander and Rover outlived their design life
- ↳ Broke all records for number of hits on a website!!!



# Remember these pictures?





## Pathfinder had Software Errors

### → Symptoms

- ↳ Software did total system resets
  - Symptoms noticed soon after Pathfinder started collecting meteorological data
  - Some data lost each time

### → Cause

- ↳ 3 Process threads, with bus access via mutual exclusion locks (mutexes):
  - High priority: Information Bus Manager
  - Low priority: Meteorological Data Gathering Task
  - Medium priority: Communications Task
- ↳ Priority Inversion:
  - Low priority task gets mutex to transfer data to the bus
  - High priority task blocked until mutex is released
  - Medium priority task pre-empts low priority task
  - Eventually a watchdog timer notices Bus Manager hasn't run for some time...

### → Factors

- ↳ Very hard to diagnose:
  - Hard to reproduce
  - Need full tracing switched on to analyze what happened
- ↳ Was experienced a couple of times in pre-flight testing
  - Never reproduced or explained
  - Hence testers assumed it was a hardware glitch



## Mars Climate Orbiter

### → Launched

- ↳ 11 Dec 1998

### → Mission

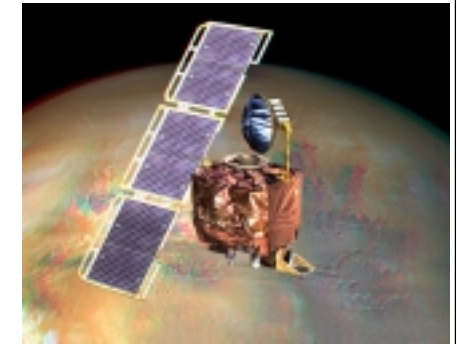
- ↳ interplanetary weather satellite
- ↳ communications relay for Mars Polar Lander

### → Fate:

- ↳ Arrived 23 Sept 1999
- ↳ No signal received after initial orbit insertion

### → Cause:

- ↳ Faulty navigation data caused by failure to convert imperial to metric units



## Small Forces...

### → Locus of error

- ↳ Ground software file called "Small Forces" gives thruster performance data
- ↳ This data used to process telemetry from the spacecraft
  - Spacecraft signals each Angular Momentum Desaturation (AMD) maneuver
  - Small Forces data used to compute effect on trajectory
  - Software underestimated effect by factor of 4.45

### → Cause of error

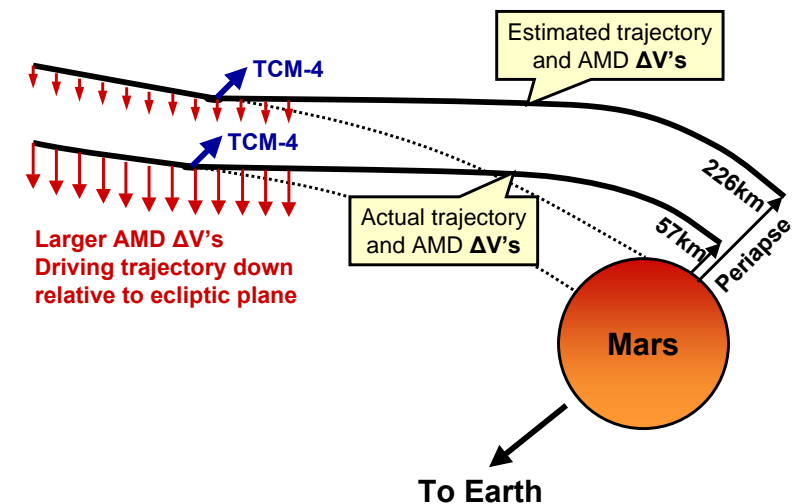
- ↳ Small Forces Data given in Pounds-seconds (lbf-s)
- ↳ The specification called for Newton-seconds (N-s)

### → Result of error

- ↳ As spacecraft approaches orbit insertion, trajectory is corrected
  - Aimed for periapse of 226km on first orbit
- ↳ Estimates were adjusted as the spacecraft approached orbit insertion:
  - 1 week prior: first periapse estimated at 150-170km
  - 1 hour prior: this was down to 110km
  - Minimum periapse considered survivable is 80km
- ↳ MCO entered Mars occultation 49 seconds earlier than predicted
  - Signal was never regained after the predicted 21 minute occultation
  - Subsequent analysis estimates first periapse of 57km



## MCO Navigation Error





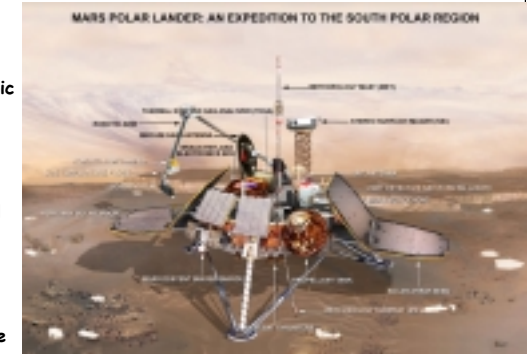
## Contributing Factors

- For 4 months, AMD data not used due to file format errors
  - ⊗ Navigators calculated data by hand
  - ⊗ File format fixed by April 1999
  - ⊗ Anomalies in trajectory became apparent almost immediately
- Limited ability to investigate:
  - ⊗ Thrust effects measured along line of sight using doppler shift
  - ⊗ AMD thrusts are mainly perpendicular to Earth-spacecraft line of sight
- Poor communication between teams:
  - ⊗ E.g. Issue tracking system not properly used by navigation team
    - Anomalies not properly investigated
- Inadequate staffing
  - ⊗ Operations team monitoring three missions simultaneously (MGS, MCO and MPL)
- Operations Navigation team unfamiliar with spacecraft
  - ⊗ Different team from development & test
  - ⊗ Did not fully understand the significance of the anomalies
  - ⊗ Familiarity with previous mission (MGS) assumed sufficient:
    - but AMD was performed 10-14 times more often on MCO as it has asymmetric solar panels.
- Inadequate Testing
  - ⊗ Software Interface Spec not used during unit testing of small forces s/w
  - ⊗ End-to-end test of ground software never completed
  - ⊗ Ground software was not considered "mission critical" so less rigorous V&V
- Inadequate Reviews
  - ⊗ Key personnel missing from critical design reviews



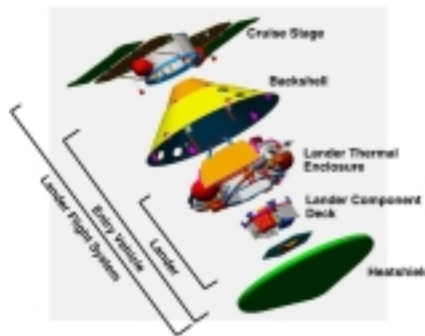
## Mars Polar Lander

- Launched
  - ⊗ 3 Jan 1999
- Mission
  - ⊗ Land near South Pole
  - ⊗ Dig for water ice with a robotic arm
- Fate:
  - ⊗ Arrived 3 Dec 1999
  - ⊗ No signal received after initial phase of descent
- Cause:
  - ⊗ Several candidate causes
  - ⊗ Most likely is premature engine shutdown due to noise on leg sensors



## What happened?

- Investigation hampered by lack of data
  - ⊗ spacecraft not designed to send telemetry during descent
  - ⊗ This decision severely criticized by review boards
- Possible causes:
  - ⊗ Lander failed to separate from cruise stage (plausible but unlikely)
  - ⊗ Landing site was too steep (plausible)
  - ⊗ Heatshield failed (plausible)
  - ⊗ Loss of control due to dynamic effects (plausible)
  - ⊗ Loss of control due to center-of-mass shift (plausible)
  - ⊗ Premature Shutdown of Descent Engines (most likely!)
  - ⊗ Parachute drapes over lander (plausible)
  - ⊗ Backshell hits lander (plausible but unlikely)



## Premature Shutdown Scenario

- Cause of error
  - ⊗ Magnetic sensor on each leg senses touchdown
  - ⊗ Legs unfold at 1500m above surface
    - transient signals on touchdown sensors during unfolding
    - software accepts touchdown signals if they persist for 2 timeframes
    - transient signals likely to be long enough on at least one leg
- Factors
  - ⊗ System requirement to ignore the transient signals
    - But the software requirements did not describe the effect
    - s/w designers didn't understand the effect, so didn't implement the requirement
  - ⊗ Engineers present at code inspection didn't understand the effect
  - ⊗ Not caught in testing because:
    - Unit testing didn't include the transients
    - Sensors improperly wired during integration tests (no touchdown detected!)
    - Full test not repeated after re-wiring
- Result of error
  - ⊗ Engines shut down before spacecraft has landed
    - When engine shutdown s/w enabled, flags indicated touchdown already occurred
    - estimated at 40m above surface, travelling at 13 m/s
    - estimated impact velocity 22m/s (spacecraft would not survive this)
    - nominal touchdown velocity 2.4m/s



## Deep Space 2

### → Launched

- ↳ 3 Jan 1999

### → Mission

- ↳ 2 small probes piggybacked on Mars Polar Lander
- ↳ Demonstration of new technology
- ↳ Separate from MPL 5 minutes before atmosphere entry
- ↳ Bury themselves in Martian Soil
- ↳ Return data on soil analysis and look for water



### → Fate:

- ↳ No signals were received after launch

### → Cause:

- ↳ Unknown
- ↳ (System was not ready for launch)



Factor	STS 51L	Ariane 501	Pathfinder	MCO	MPL	DS-2
Didn't test to spec		●		●	●	?
Insufficient test data	●	●			●	●
Tested "wrong" system					●	
No regression test					●	
Lack of integration testing		●		●		●
Lack of expertise at inspections		●		●	●	
System changed after testing					●	?
Req't not implemented		?		●	●	
Lack of diagnostic data during ops			●	●	●	●
S/W used before ready				?	?	●
Different team maintains S/W				●	●	
Didn't use problem reporting system	●		●	●	●	?
Didn't track problems properly	●	●	●	●	●	?
Didn't investigate anomalies	●		●	●		
Poor communication between teams	●	●	●	●	●	?
Insufficient staffing	●			●	●	●
Failure to adjust budget and schedule	●			●	●	●
Inexperienced managers	?			●	●	●
Commercial pressures took priority	●	●		●	●	●
reused code w/o checking assumptions		●				
'Redundant' design not redundant	●	●				



## Summary

### → Failures can usually be traced to a single root cause

- ↳ But good engineering practice should prevent these causing system failure
- ↳ The real problems are failures of:
  - > testing and inspection process
  - > problem reporting and tracking
  - > lack of expertise
  - > inadequate resources
  - > etc...

- ↳ In most cases, it takes a failure of both engineering practice and of management

### → Reliable software depends not on flawless programs but on how good we are at:

- ↳ Communication (sharing information between teams)
- ↳ Management (of Resources and Risk)
- ↳ Verification and Validation
- ↳ Risk Identification and tracking
- ↳ Questioning assumptions



## Resource List

### → Mars Observer

- ↳ Project summary
  - > [http://www.msss.com/mars/observer/project/mo\\_loss/moloss.html](http://www.msss.com/mars/observer/project/mo_loss/moloss.html)
- ↳ Brief summary of possible causes
  - > <http://catless.ncl.ac.uk/Risks/14.89.html#subj1>

### → Mars Pathfinder

- ↳ Project info:
  - > <http://mars.jpl.nasa.gov/MPF/index1.html>
- ↳ Report on the priority inversion problem:
  - > <http://catless.ncl.ac.uk/Risks/19.49.html#subj1>

### → Mars Climate Orbiter

- ↳ Project Info:
  - > <http://mars.jpl.nasa.gov/msp98/orbiter/>
- ↳ Investigation Report:
  - > [ftp://ftp.hq.nasa.gov/pub/pao/reports/2000/MCO\\_MIB\\_Report.pdf](ftp://ftp.hq.nasa.gov/pub/pao/reports/2000/MCO_MIB_Report.pdf)

### → Mars Polar Lander & Deep Space 2

- ↳ Project info:
  - > <http://mars.jpl.nasa.gov/msp98/lander/>
  - > <http://mars.jpl.nasa.gov/msp98/ds2/>
- ↳ Investigation Reports:
  - > <http://www.nasa.gov/newsinfo/marsreports.html>

### → General Resources

- ↳ JPL's list of missions (past, present and future)
  - > [http://www.jpl.nasa.gov/missions/missions\\_index.html](http://www.jpl.nasa.gov/missions/missions_index.html)
- ↳ Basics of Space Flight:
  - > <http://www.jpl.nasa.gov/basics/>